UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/916,785	07/27/2001	Gadiel Seroussi	10010554-1	8810

7590 03/28/2005

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80528-9599

EXAMINER	
KHAN, ASHFAQ M	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 03/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/916,785	SEROUSSI ET AL.	
	Examiner	Art Unit	
	Ashfaq Khan	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *Three* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 March 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9* is/are rejected.

7)☒ Claim(s) *1 and 2* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *12/23/2003*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Remarks

Claims 1-9 are pending.

Claim Objection

The third paragraph of both Claim 1 and 2 has been objected. There is no mention about 'circuit' and 'merge circuit' in the drawing as well. It's not clear whether these are the same element or the different one, therefore has been objected.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) The invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claim 1 has been rejected under 35 U.S.C. 102(b) as being anticipated by Eastlake et al. - Randomness Recommendations for Security, RFC – 1750, December 1994, Page 1 – 30 (hereinafter Eastlake).

As per claim 1 Eastlake discloses a random number generator comprising:

A first sensor for generating a first sequence of digital values representing measurements of a first environmental quantity at successive times; (Page 10 section 5.0, A thermal noise is represented as first environmental quantity, where a first sensor inherently measures the thermal noises).

A first compressor for compressing said first sequence of digital values to provide a first sequence of compressed values having a lower internal correlation than said values of said first sequence of digital values; (Page 10 section 5.2 and Page 13 section 5.2.4 - showing de-skewing digital values using compression).

A circuit for generating a random number from an input sequence of digital values, said input sequence being a function of one of said first sequence of compressed values (Page 14-15 section 6.0, Page 19 section 6.2 – Mixture for mixing digital values generated from the thermal noise source with other uncorrelated source's values).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 2 has been rejected under 35 U.S.C. 103(a) as being unpatentable over Eastlake in view of Ritter, T. – The Hardware Random Number Generator: A Ciphers By Ritter Page, www.ciphersbyritter.com/NEWS4/HARDRAND.HTM, January 25, 1999 Page 1- 145.

Regarding claim 2, Eastlake's memo teaches the invention substantially as claimed. See the rejection of claim 1 above. More specifically Eastlake teaches that a mixture using trivial mixing function taking uncorrelated inputs 1 and 2 to generate a less skewed random bit (Page 15 section 6.1.1). The claim does not teach about utilization of a second sensor and compressor.

However, Ritter's posted web conversation recognizes that the system should have redundant systems that are combined to give the final random number (Page 22 paragraph 4). From the several choices of hardware randomness presented in Eastlake's memo the radioactive decay source could be represented as second environmental quantity, where a second sensor inherently will measure the decay (Page 10 section 5.0).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Ritter's teaching of utilizing redundant systems to generate random numbers with Eastlake's teaching because this is the best possible way of generating unpredictable random number (Ritter - Page 22 paragraph 4).

Claim 3 has been rejected under 35 U.S.C. 103(a) as being unpatentable over Eastlake in view of Ritter, T. – The Hardware Random Number Generator: A Ciphers By Ritter Page,

www.ciphersbyritter.com/NEWS4/HARDRAND.HTM, January 25, 1999 Page 1- 145, and further in view of Individual Logic Gates and De Morgan's Theorem, www.ece.msstate.edu/classes/ece3281/lab/3281exp8.doc, October 16th, 2000, Page 1- 10 (hereinafter Lgate)

Regarding claim 3, Eastlake's memo teaches the invention substantially as claimed. See the rejection of claim 1 and 2 above. However, Eastlake does not teach about the merge circuit mentioned in claim 2, also comprises a third compressor.

According to Lgate, two inputs DS-1 and DS-2 generates an output DI-1 after passing through the 'and' gate. DI-1 and input Ds-3 is then pass through the 'and' gate and generate the second output DI-2. Similar Mixture using trivial mixing function as per Eastlake's teaching of claim 2 could be utilized to a less skewed random bit for the output DI-2 (Eastlake - Page 15 section 6.1.1).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the Lgate's teaching of utilizing combination of multiple inputs with the combination of Eastlake's teaching in view of Ritter's page because output generated using multiple uncorrelated inputs combined in this way will increase the randomness even more (Eastlake - Page 15 section 6.1.1).

Claim 4 has been rejected under 35 U.S.C. 103(a) as being unpatentable over Eastlake in view of Saito (US Patent# 6,542,014 B1).

Regarding Claim 4, Eastlake's memo teaches the invention substantially as claimed. See the rejection of claim 1 above. However, Eastlake does not teach any utilization of environmental quantity as temperature to generate random number.

According to Saito's invention a thermal noise generating element (Fig 1 – Item 2) has been utilized for random number generation.

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the Saito's teaching of utilizing thermal noise generating element with Eastlake's teaching because this way it is possible to generate the true physical random numbers at a required speed by utilizing random number generator with a simple configuration with known inexpensive electronic parts (Col 1 Line 61-65).

Claim 5 has been rejected under 35 U.S.C. 103(a) as being unpatentable over Eastlake in view of Dultz et al. (US Patent# 6,609,139 B1).

Regarding Claim 5, Eastlake's memo teaches the invention substantially as claimed. See the rejection of claim 1 above. However, Eastlake does not teach any utilization of environmental quantity as light level to generate random number.

According to Dultz's invention describes generating random numbers on a quantum-mechanics utilizing a fundamental choice of path of a quantum particle on a beam splitter (Col 3 line 66 – Col 4 line 9).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the Dultz's teaching splitting of beam splitter for generating random number with Eastlake's teaching because as many as possible particles emitted by the particle source result in a usable counting event at the detector. The counting probability is increased, thus building a fast reliable random sequence (Col 3 line 60 – 65).

Claim 6 has been rejected under 35 U.S.C. 103(a) as being unpatentable over Eastlake in view of Vincze et al. (US Patent# 6,369,727 B1).

Regarding Claim 6, Eastlake's memo teaches the invention substantially as claimed. See the rejection of claim 1 above. However, Eastlake does not teach any utilization of environmental quantity as acoustical level to generate random number.

According to Vincze's invention describes generating random number by utilizing a noise source (Fig 1 - item 21, Col 3 line 20-34).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the Vincze's teaching of random number generation by utilizing a sound source with Eastlake's teaching because this way it is possible to generate random number sequence that is automatic and free of radiological consideration (Col 3 line 15 – 18).

Claim 7 has been rejected under 35 U.S.C. 103(a) as being unpatentable over Eastlake in view of Larson et al. (US Patent# 4,641,840).

Regarding Claim 7, Eastlake's memo teaches the invention substantially as claimed. See the rejection of claim 1 above. However, Eastlake does not teach any utilization of environmental quantity as measurement of motion to generate random number.

According to Larson's invention describes random number generation by utilizing detection of motion with a motion-switch (Fig 1 - item 40, Col 4 line 8-27).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the Vincze's teaching of random number generation utilizing motion detection with Eastlake's teaching because according to Larson this electronically operating playing die will increase the excitement of the game by the interaction of the die rolling and the random number generation of the electronic circuit (Col 2 line 34- 40).

Claim 8 has been rejected under 35 U.S.C. 103(a) as being unpatentable over Eastlake in view of Buhler et al (EP 1 081 591 A2).

Regarding Claim 8, Eastlake's memo teaches the invention substantially as claimed. See the rejection of claim 1 above. However, Eastlake does not teach any utilization of hash function on the random number generation circuit.

However Buhler's invention describes implementation of standard hashing algorithms in random number generation process (Col 1 paragraph 4, Col 7 paragraph 28).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the Buhler's implementation of hashing in random number generation with Eastlake's teaching because the data integrity is achieved through the use of hash-value generated from hash function.

Claim 9 has been rejected under 35 U.S.C. 103(a) as being unpatentable over Eastlake in view of Chan et al (US Patent# 6,046,616).

Regarding Claim 9, Eastlake's memo teaches the invention substantially as claimed. See the rejection of claim 1 above. However, Eastlake does not teach any blocking mechanism for preventing the random number generation.

However Chan's invention implements a 'hold signal' for allowing and preventing random number generation (Col 5 line 6 - 12).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the Chan's implementation of holding the random number generation during the cycle with Eastlake's teaching because the data integrity is achieved through this way by making sure that all the input signals are in the same size.

Conclusion

A shortened statutory period for response to this action is set to expire **Three months** from the mail date of this letter. Failure to respond with in the period for response will result in **ABANDONMENT** of the application (see 35 U.S.C. 133, M.P.E.P. 710.02, 710.02(b)).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ashfaq Khan whose telephone number is (571) 272-7964. The examiner can normally be reached on M-F between 9:00am - 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER